**Post Date: 2026/06/30**

# Vulnerability Alert CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2026/06/22-2026/06/28)

- Subject: Vulnerability Alert CISA Adds 6 Known Exploited Vulnerabilities to KEV Catalog (2026/06/22-2026/06/28)

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team / Coordination Center (TWCERTCC) Cybersecurity Alert: TWCERTCC-200-202606-00000018
  - CVE-2025-67038 Lantronix EDS5000 Code Injection Vulnerability (CVSS v3.1: 9.8)
  - Known Ransomware Exploitation: Unknown A code injection vulnerability exists in Lantronix EDS5000. An attacker could exploit this vulnerability to inject arbitrary operating system commands into the username parameter and execute them with root privileges.
  - CVE-2026-34910 Ubiquiti UniFi OS Improper Input Validation Vulnerability (CVSS v3.1: 10.0)
  - Known Ransomware Exploitation: Unknown An improper input validation vulnerability exists in Ubiquiti UniFi OS. A malicious attacker with network access could exploit this vulnerability to perform command injection attacks.
  - CVE-2026-34909 Ubiquiti UniFi OS Path Traversal Vulnerability (CVSS v3.1: 10.0)
  - Known Ransomware Exploitation: Unknown A path traversal vulnerability exists in Ubiquiti UniFi OS. A malicious attacker with network access could exploit this vulnerability to access files on the underlying system, and potentially gain access to underlying system accounts by manipulating or exploiting these files.
  - CVE-2026-34908 Ubiquiti UniFi OS Improper Access Control Vulnerability (CVSS v3.1: 10.0)
  - Known Ransomware Exploitation: Unknown An improper access control vulnerability exists in Ubiquiti UniFi OS. A malicious attacker with network access could exploit this vulnerability to make unauthorized changes to the system.
  - CVE-2026-12569 PTC Windchill and FlexPLM Improper Input Validation Vulnerability (CVSS v3.1: 9.8)
  - Known Ransomware Exploitation: Unknown An improper input validation vulnerability exists in PTC Windchill and FlexPLM. An unauthenticated remote attacker could execute arbitrary code by sending malicious requests to the network.
  - CVE-2026-20230 Cisco Unified Communications Manager Server-Side Request Forgery (SSRF) Vulnerability (CVSS v3.1: 8.6)
  - Known Ransomware Exploitation: Unknown A server-side request forgery (SSRF) vulnerability exists in Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME). An unauthenticated remote attacker could exploit this vulnerability to write files to the underlying operating system, and subsequently utilize these files to further elevate privileges to root.
- Affected Platforms:

    - CVE-2025-67038Please refer to the official affected versions listed at: https://www.lantronix.com/technical-support/security-updates/vulnerability-disclosure-policy/vulnerability-library/cve-2025-67038-eds-5000-eds-3000/?_gl=1*11k48gn*_up*MQ..*_ga*NzY1MzgwNjcxLjE3ODI2OTc0Nzg.*_ga_M2G6RLT5L3*czE3ODI2OTc0NzckbzEkZzEkdDE3ODI2OTc1NTckajYwJGwwJGgw
    - CVE-2026-34910Please refer to the official affected versions listed at: https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
    - CVE-2026-34909Please refer to the official affected versions listed at: https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
    - CVE-2026-34908Please refer to the official affected versions listed at: https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
    - CVE-2026-12569Please refer to the official affected versions listed at: https://www.ptc.com/en/support/article/CS473270
    - CVE-2026-20230Please refer to the official affected versions listed at: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssrf-cXPnHcW
- Recommended Actions:
    - CVE-2025-67038 Official fixes and updates have been released for this vulnerability. Please update to the relevant versions at: https://www.lantronix.com/technical-support/security-updates/vulnerability-disclosure-policy/vulnerability-library/cve-2025-67038-eds-5000-eds-3000/?_gl=1*11k48gn*_up*MQ..*_ga*NzY1MzgwNjcxLjE3ODI2OTc0Nzg.*_ga_M2G6RLT5L3*czE3ODI2OTc0NzckbzEkZzEkdDE3ODI2OTc1NTckajYwJGwwJGgw
    - CVE-2026-34910 Official fixes and updates have been released for this vulnerability. Please update to the relevant versions at: https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
    - CVE-2026-34909 Official fixes and updates have been released for this vulnerability. Please update to the relevant versions at: https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
    - CVE-2026-34908 Official fixes and updates have been released for this vulnerability. Please update to the relevant versions at: https://community.ui.com/releases/Security-Advisory-Bulletin-064-064/84811c09-4cf4-42ab-bd61-cc994445963b
    - CVE-2026-12569 Official fixes and updates have been released for this vulnerability. Please update to the relevant versions at: https://www.ptc.com/en/support/article/CS473270
    - CVE-2026-20230 Official fixes and updates have been released for this vulnerability. Please update to the relevant versions at: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-ssrf-cXPnHcW

---

Computer and Communication Center
Network Systems Division

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
**https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260630_22**

Last update: **2026/06/30 09:23**